

**U.S. Department of Justice**



National Domestic Communications Assistance Center  
Executive Advisory Board  
Meeting Minutes  
November 19, 2019

---



**Appendix A**



## **National Domestic Communications Assistance Center**

### **EXECUTIVE ADVISORY BOARD**

**November 19, 2019**

#### **Call to Order – Welcome and Introduction**

Alice Bardney-Boose, *Designated Federal Officer*

#### **Remarks of Outgoing Chairman**

Preston Grubbs, *Former Chairman*

#### **Introduction of EAB Members & Chairman's Remarks**

Al Cannon, *Chairman*

#### **Lawful Access State and Local Perspective**

Ben Bawden, Brooks Bawden Moore

#### **NDCAC Update**

Marybeth Paglino, *NDCAC Director*

- Review of NDCAC activity since last meeting and planned projects

#### **2019 Report on Smartphone Encryption and Public Safety**

Kenn Kern, Manhattan District Attorney's Office

#### **Report of the Administrative Subcommittee**

Hank Stawinski, *Subcommittee Chairman*

- Member Status, EAB Leadership, Charter renewal

#### **Report of the Technology Subcommittee**

Michael Sachs, Subcommittee Chairman

- Activity since last meeting

#### **Lawful Access and the NDCAC's Role**

David Bowdich, FBI

#### **Acknowledgement of Submitted Comments**

Al Cannon, *Chairman*

#### **Establishing EAB Schedule of Future Meetings**

Alice Bardney-Boose, *Designated Federal Officer*

#### **Adjournment**



## U.S. Department of Justice

### National Domestic Communications Assistance Center Executive Advisory Board

NDCAC EAB State and Local Members		
Name	Title	Organization
James A Cannon, Chair*	Sheriff, Charleston County Sheriff's Office	Major County Sheriffs
Mark A. Keel	Chief, South Carolina Law Enforcement Division	Association of State Criminal Investigative Agencies
Lenny Millholland	Sheriff, Frederick County Sheriff's Office	National Sheriffs Association
Christopher Noelck	Special Agent in Charge, Investigative Operations, Iowa Department of Public Safety	National Narcotics Officers' Associations' Coalition
Thomas G. Ruocco	Assistant Director/Chief, Criminal Investigations Division, Texas Department of Public Safety	International Association of Chiefs of Police
Michael Sachs	Executive Assistant District Attorney, County of New York District Attorney's Office	Association of Prosecuting Attorneys
Henry Stawinski	Chief of Police, Prince George's County	Major City Chiefs
Edwin Zabin	First Assistant District Attorney, Suffolk County District Attorney's Office	National District Attorney's Association
NDCAC EAB Federal Members		
Name	Title	Organization
David Bowers	Inspector in Charge, Security & Crime Prevention	US Postal Inspection Service
Michael D'Ambrosio	Deputy Assistant Director, Office of Investigations	US Secret Service
Alysa Erichs	Assistant Director, Information Management	Immigration and Customs Enforcement
G. Clayton Grigg	Deputy Assistant Director, Laboratory Division	Federal Bureau of Investigation
Timothy Plancon**	Assistant Administrator, Operations Support	Drug Enforcement Administration
Jeffrey Tyler**	Assistant Director, Investigative Operations Division	US Marshals Service
Paul Vanderplow	Chief, Special Operations Division	Bureau of Alcohol, Tobacco, and Firearms
NDCAC EAB Non-Voting Members		
Name	Title	Organization
Alice Bardney-Boose	Designated Federal Officer	Federal Bureau of Investigation
Marc Labreche	Attorney, Office of the General Counsel (OGC)	Federal Bureau of Investigation
Peter Winn	Chief Privacy and Civil Liberties Officer, ODAG	Department of Justice

\* Mr. Cannon became Chair effective November 4, 2019, when the Attorney General approved a new EAB member representing the DEA (see note below). The Vice Chair position is currently vacant.

\*\* Recent member additions: Mr. Plancon replaced Mr. Preston Grubbs, Principal Deputy Administrator, DEA, previous EAB Chair; and Mr. Tyler replaced Mr. Derrick Driscoll, Deputy Director, USMS.

**U.S. Department of Justice**

National Domestic Communications Assistance Center  
Executive Advisory Board  
Meeting Minutes  
November 19, 2019



---

**Appendix B**





REPORT OF THE  
MANHATTAN DISTRICT ATTORNEY'S  
OFFICE ON

SMARTPHONE  
ENCRYPTION  
*and* PUBLIC SAFETY

*An update to the November 2018 Report*

October 2019

Kenn Kern

National Domestic Communications Assistance Center  
Executive Advisory Board

November 19, 2019

# Outline for Today

- I. Quantitative Analysis
- II. Qualitative Analysis
- III. International Developments / Coordination
- IV. Changing Political and Regulatory Climate
- V. Senate Judiciary Committee Hearing

# Apple and Smartphone Encryption



## What we're most commonly asked for and how we respond.

The most common requests we receive for information come from law enforcement in the form of either a Device Request or an Account Request. Our legal team carefully reviews each request, ensuring it is accompanied by valid legal process. All content requests require a search warrant. Only a small fraction of requests from law enforcement seek content such as emails, photos, and other content stored on users' iCloud or iTunes account. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category altogether.

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Source: <https://www.apple.com/privacy/government-information-requests>

In September 2014, **Apple** engineered its new mobile operating system, iOS 8, so that it can no longer assist law enforcement with search warrants written for locked devices.

Source: <https://www.apple.com/privacy/government-information-requests>



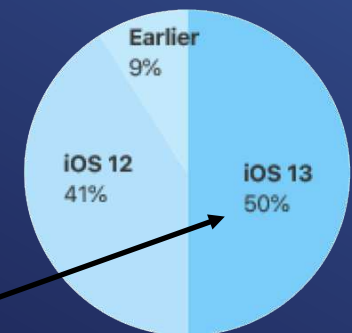
**Google**, maker of the Android operating system, quickly announced plans to follow suit.

Source: <http://officialandroid.blogspot.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html>



Apple and Google's operating systems run a combined **99.9% of smartphones** worldwide.

Source: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>



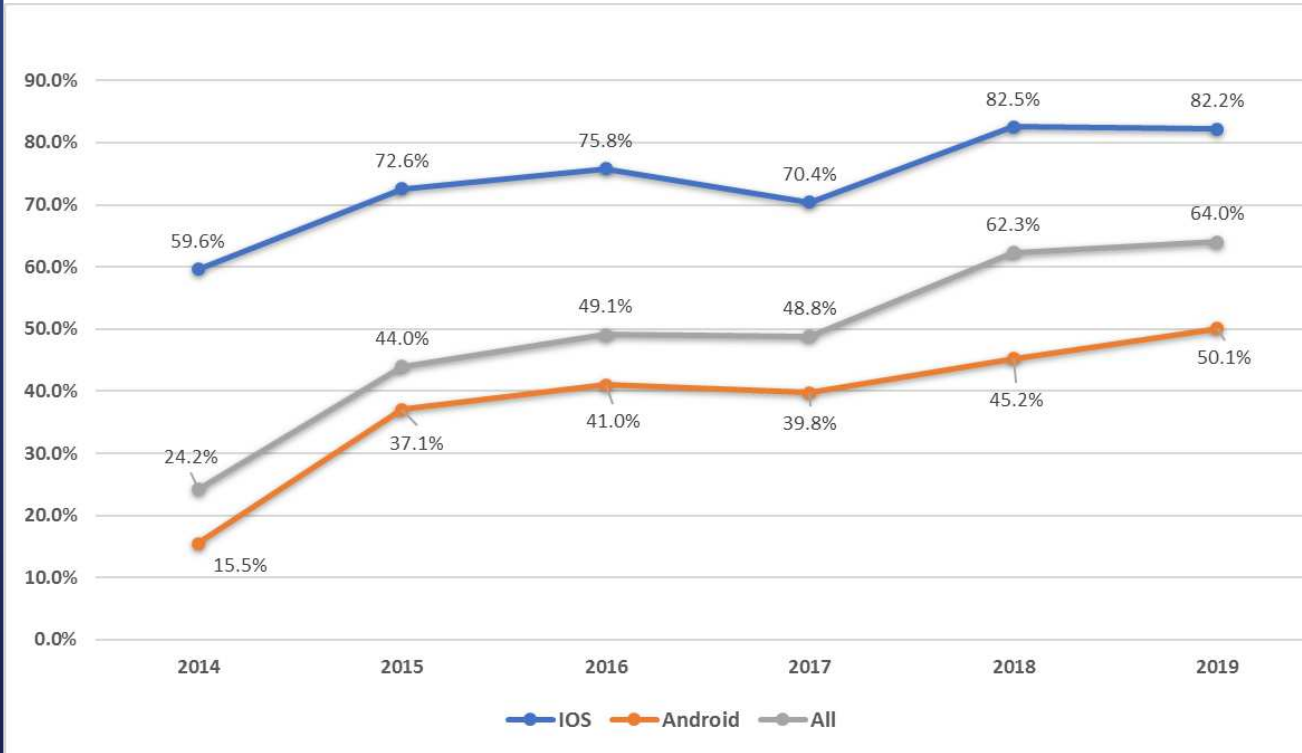
As of October 15, 2019, 50 percent of all Apple devices are running iOS 13 or newer.

Source: <https://developer.apple.com/support/app-store>

At the Manhattan DA's Office alone, **over 2,500** lawfully-obtained iPhones since 2014 were inaccessible when they were seized. In 2019 alone, **over 82%** of all Apple devices received by our digital forensics unit were locked.

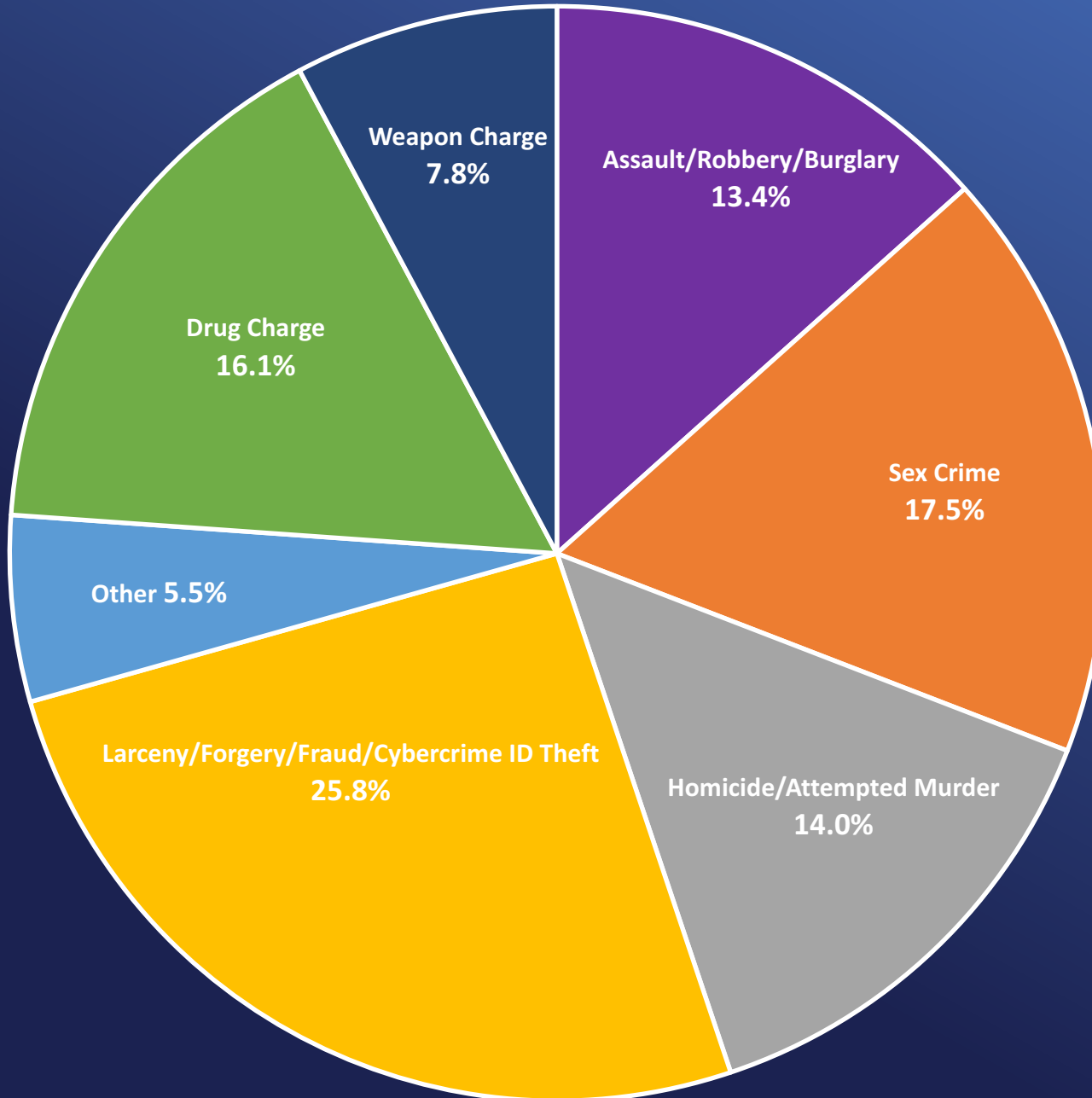
These devices represent hundreds of real crimes against New Yorkers that cannot be fully investigated, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

**Rate of Locked Devices Upon Arrival**  
2014 - 2019



# Crime Type of All Mobile Devices

January 1, 2019 - September 1, 2019





# Value of Ability to Access Devices

Question: What was the impact of the ability to unlock the device?

(3) What was the impact of the ability to unlock the device (to the best of your assessment)? (check all that apply)  
*Note: if box checked, please describe how device access contributed.*

- ☐ Arrest made
- ☐ Additional or elevated charges brought
- ☐ Led to opening new investigation
- ☐ Identification of co-conspirators or accomplices
- ☒ Provided additional evidence that improved the strength of the case

The case was purely circumstantial before the evidence from the phone was obtained. The video footage was not clear, and no witness could actually provide a confident ID of the defendant using the video. Further, the incident was reported long after the time ECT could salvage any actual DNA/biological evidence or link the defendant to the crime. The phone provided the people with the defendant's conversations, which had near-

- ☐ Exonerated target, co-defendant, or other party
- ☐ Other

- 17 cases where evidence on a locked phone ultimately exonerated and/or mitigated the culpability of a target or co-defendant





# Value of Ability to Access Devices: Exoneration / Mitigation

- “**Phone corroborated** owner's statement that he had not been present when shots were fired”
- “The **information** in this decedent's phone **demonstrated** that he died of a voluntary drug overdose.”
- “One **video depicts** defendant using PCP on night of murder, which is **consistent** with **defense** theory of NGRI”
- “**Corroborated defendant's statements** that he was not present at the time of the crime in a one witness identification case”



# Measuring the Effect of Encryption on Cases

- “Defendant and 2 others are alleged to have entered the victim's apartment and robbed him at gunpoint. Our **inability to access** the contents phone **prevents** us from seeing who he was in contact with before, during, or directly following the offense. While we can subpoena phone records, there is no other means to access text information or internet based communications such as FaceTime, WhatsApp, Facebook Messenger calls, etc.”
- “Defendant is seen **using** his **phone** immediately **after** the charged **murder**. Phone may have contained admissions going to defendant's state of mind and his justification defense.”
- “Case investigated by sex crimes as unlawful surveillance, it was **reduced** to a misdemeanor because we **could not access** the **phone**.”





# Value of Ability to Access Devices

## SEX CRIMES & CHILD PORNOGRAPHY

- “From the defendant's phone we **obtained 3 videos** which constituted CP and we brought a **new indictment** charging him with Promoting a Sexual Performance by a Child, Use of a Child in a Sexual Performance, Possessing a Sexual Performance by a Child, and Unlawful Surveillance.

These videos were also **strong corroboration** of the CW's narrative in which she described the defendant entering her bedroom at night and raping her since the videos were all filmed during the night, in her bedroom, while she was sleeping and unaware.”



# Value of Ability to Access Devices

## MURDER

- “This was a murder prosecution. Phone evidence provided (1) motive for crime, (2) partial admission to crime, (3) ability to conduct full investigation into potential cooperator before signing agreement.”
- “Phone contained admissions by defendant that he possessed a firearm days before the shooting murder.” Phone showed D efforts to hide following the crime. Phone connected D to the individuals captured on video with the murderer at the time of the crime.”



# International Developments

## Australia:

- *“The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill (“AAB”)*

now establishes a framework for both voluntary and mandatory industry assistance to Australian law enforcement and intelligence agencies that is to be triggered by a governmental notice. Such notices may be issued to any entity that provides online services or communications equipment within Australia (e.g., websites, applications, and telecom companies), and may compel the recipient to undertake a number of actions ranging from removing forms of electronic protection that they themselves have applied, to installing and using certain software or equipment.



# International Developments

## The European Union:

- In January 2019, Europol released, *A First Report of the Observatory Function on Encryption*.

This new report explicitly recognizes that the current debate about encryption has become too polarized, with tech companies unnecessarily framing the issue as a “zero-sum game,” in which any tool that provides lawful access to law enforcement will necessarily compromise user privacy. To break this logjam, the EU advocates “targeted approaches” to the development of new investigative tools that are “proportionate to the crime that was committed.” This approach is consistent with the European Commission’s prior commitment to research “functional encryption:” technologies that would change the way data is encrypted in the first place, to allow law enforcement to gain selective access to data in certain circumstances, instead of granting “all or nothing” law enforcement access to a device.



# The “Five Eyes”



- In the summer of 2019, the Five Eyes members held a conference in which senior ministers met to discuss ways of coordinating with the tech sector on encryption.
- Among the key themes was the need for international coordination in the face of emerging threats. Speaking at the conclusion of the conference, United States Attorney General William Barr noted that, “making our virtual world more secure should not come at the expense of making us more vulnerable in the real world.” Following the conference, the group released a statement reaffirming its commitment to pursuing lawful access to encrypted devices.

## Facebook Encryption Eyed in Fight Against Online Child Sex Abuse

An explosion in reports of child sexual abuse imagery on the internet is prompting the authorities to step up pressure on technology companies over their use of encryption — and Facebook, which flags by far the largest amount of the material, is drawing outsize attention.

There is increasing “international consensus, at least among law enforcement folks, that this is a serious problem,” said Sujit Raman, an associate deputy attorney general in the Justice Department. “And the companies, you know, they’re just not as engaged on the issue as they really need to be.”

The New York Times reported on Saturday that Facebook Messenger, which is not encrypted, accounted for nearly two-thirds of reports last year of online child sexual abuse imagery. On Wednesday, the Justice Department said that Facebook as a whole was responsible for 90 percent of the reports.

In March, the company’s chief executive, Mark Zuckerberg, announced that the messaging service [would move to encryption](#) in coming years, setting up a direct conflict between its business interests and the demands of law enforcement.

Justice Department officials, including Attorney General William P. Barr, are expected to raise concerns about the change to Messenger, and about encryption overall, at [an event on Friday](#) with the Federal Bureau of Investigation, the national clearinghouse for child sexual abuse imagery and officials from the Australia and Britain.

“Online child exploitation has increased dramatically in the past few years, and offenders continue to adopt more sophisticated means to entice victims and evade justice,” the department said in invitations to the event.

By Jennifer Valentino-DeVries and Gabriel J.X. Dance

Oct. 2, 2019

## US, UK, and Australia jointly request for Facebook to stop end-to-end encryption plans

Trio call for Facebook to allow law enforcement to obtain lawful access to content in a readable and usable format.

The United States, the United Kingdom, and Australia have joined to request that Facebook delay its plans to implement end-to-end encryption across its messaging services.

First reported by [BuzzFeed News](#), the governments on Thursday jointly published an open letter to Facebook CEO Mark Zuckerberg, asking for the company to ensure that encryption does not impede government officials from investigating possible crimes.

The letter was jointly signed by US Attorney General, William Barr; UK Home Secretary, Priti Patel; Australian Home Affairs Minister, Peter Dutton; and the US acting Secretary of Homeland Security, Kevin McAleenan.

The letter to Facebook said that companies "should not deliberately design their systems to preclude any form of access to content" as the governments believe encryption will put citizens and societies at risk of child sexual exploitation and abuse, terrorism, and foreign interference.

"Security enhancements to the virtual world should not make us more vulnerable in the physical world," the letter added.

It calls for Facebook to allow law enforcement to obtain lawful access to content in a readable and usable format; engage in consultation with governments to facilitate lawful access and allow this to influence Facebook’s design decisions; and to not implement any encryption changes.

This is despite the governments acknowledging that Facebook -- along with WhatsApp, Facebook Messenger, and Instagram -- have captured 99% of the child sexual exploitation and terrorist content that reside on its platforms.

By Campbell Kwan | October 4, 2019 -- 04:00 GMT (21:00 PDT) |  
Topic: Security

## FBI director claims encryption plan would make Facebook a 'dream come true' for child pornographers

**Washington (CNN)** — FBI Director Christopher Wray said [Facebook](#) is at risk of becoming a "dream come true" for child pornographers if it follows through with a plan to encrypt all of its users' messages.

"This is incredibly concerning, to put it mildly," Wray said in a speech at the Justice Department Friday morning. "When it comes to protecting children we're at a real inflection point and we risk falling off the cliff."

The swipe at the social media giant came as law enforcement officials have redoubled their efforts against a trend by technology companies towards data privacy that has hampered police abilities to access potential evidence.

On Friday, at the start of a full day conference on encryption and child abuse, Wray described how images and video of child pornography traded between abusers on Facebook -- critical elements in building a child pornography case -- could be lost if the platform encrypted communications.

Currently, Facebook is the main provider of leads to the National Center for Missing & Exploited Children, sending more than 90% of the 18 million referrals the agency gets every year, Wray said.

But under Facebook's proposed privacy plan, the company will lose avenues to see the content of those messages, restricting access to only certain pieces of metadata, like where and when messages are sent. That's expected to reduce the number of tips they send in by 70%, the Justice Department says.

"We will find ourselves laboring only on the tip of the iceberg, working on a small number of cases that authorities actually learn about, while the vast bulk of the kids who really need us then remain out of view hidden below," Wray said.

"Facebook would transform from the main provider of child exploitation tips to a dream come true for predators and child pornographers: a platform that allows them to find and connect with kids and like-minded criminals with little fear of consequences," he said.

"We are seeking a front door," Barr said. "We would be happy if the companies providing the encryption keep the keys. What we are asking is that some responsible party have the keys so that when we can demonstrate a lawful basis - probable cause that crimes are being committed - we can gain access to that evidence."

CNN's Kevin Collier contributed to this report.

By David Shortell, CNN  
Updated 3:22 PM ET, Fri October 4, 2019



## Exclusive: Interpol plans to condemn encryption spread, citing predators, sources say

Joseph Menn



SAN FRANCISCO (Reuters) - The international police organization Interpol plans to condemn the spread of strong encryption in a statement Monday saying it protects child sex predators, three people briefed on the matter told Reuters.

At the group's conference in Lyon, France on Friday, an Interpol official said a version of the resolution introduced by the U.S. Federal Bureau of Investigation would be released without a formal vote by representatives of the roughly 60 countries in attendance, the sources said.

Echoing a joint letter last month from the top law enforcement officials in the United States, United Kingdom and Australia, the larger group will cite difficulties in catching child sexual predators as grounds for companies opening up user communications to authorities wielding court warrants.



FILE PHOTO: A man passes an Interpol logo during the handing over ceremony of the new premises for Interpol's Global Complex for Innovation, a research and development facility, in Singapore September 30, 2014.

REUTERS/EDGAR SU/FILE PHOTO

"Service providers, application developers and device manufacturers are developing and deploying products and services with encryption which effectively conceals sexual exploitation of children occurring on their platforms," a draft of the resolution seen by Reuters said.

"Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and useable format."

Interpol did not respond to a request for comment Sunday. The FBI referred questions to Interpol.

The cooperative law enforcement association is best known for helping countries assist one another in catching suspects outside their jurisdictions. The new statement will not have the force of law, but instead aim at increasing pressure on tech providers.

It could provide greater political cover for more countries to pass laws or regulations barring unbreakable encryption or requiring companies to be capable of hacking their own users, both of which are anathema to major U.S.-based global providers including Apple and Google.

Both the United Kingdom and Australia have recently passed laws moving in that direction, though it is unclear how widely they are being wielded. U.S. skirmishes have been fought in sealed court proceedings, without major congressional action.



# The Changing Political and Regulatory Climate

- “Facebook has said, ‘Just trust us,’ . . . And every time Americans trust you, they seem to get burned.” – Senator Sherrod Brown (D-Ohio).
- “I don’t trust you guys.” – Senator Martha McSally (R-Arizona) (referring to Facebook).
- “Clearly, our trust and patience in your company and your monopoly has run out[.]” – Senator Josh Hawley (R-Missouri) (regarding Google).
- “You can be an umpire or you can own teams, but you can’t be an umpire and own one of the teams that’s in the game.” – Senator Elizabeth Warren (D-Massachusetts) (regarding “Big Tech”).
- “We cannot allow giant companies to assert their power over critical public infrastructure.” – Senator Mike Crapo (R-Idaho) (regarding Facebook).



---

Senate Judiciary Committee Hearing  
December 10, 2019

---

---

# Kenn Kern

Chief Information Officer

Special Assistant for International Relations

Executive Management Central

New York County District Attorney's Office

[www.manhattanda.org](http://www.manhattanda.org)

[www.globalcyberalliance.org](http://www.globalcyberalliance.org)

---

**U.S. Department of Justice**

National Domestic Communications Assistance Center  
Executive Advisory Board  
Meeting Minutes  
November 19, 2019



---

**Appendix C**

**CHARTER**  
**U.S. DEPARTMENT OF JUSTICE**  
**NATIONAL DOMESTIC COMMUNICATIONS ASSISTANCE CENTER**  
**Executive Advisory Board**

1. **Committee's Official Designation (Title):** The Committee shall be known as the National Domestic Communications Assistance Center (NDCAC) Executive Advisory Board (hereafter referred to as the Board).
2. **Authority:** Establishment of the Board is approved at the discretion of the Attorney General. The Board is being established in accordance with the provisions of the Federal Advisory Committee Act (FACA), as amended, 5 U.S.C. App. 2.
3. **Objectives and Scope of Activities:** The Board will provide advice and recommendations to the Attorney General or his designee, and to the Director of the NDCAC that will promote public safety and national security by advancing the NDCAC's core functions: law enforcement coordination with respect to technical capabilities and solutions, technology sharing, industry relations, and implementation of the Communications Assistance for Law Enforcement Act (CALEA). Specifically, the Board will provide advice and recommendations to the Attorney General or his designee on: 1) the selection and appointment of the Director and Deputy Director(s) of the NDCAC; 2) trends and developments with respect to existing and emerging communications services and technologies; 3) technical challenges faced by Federal, State, tribal and local law enforcement agencies with respect to lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities; 4) the effective leveraging and exchange of technical information and methods among Federal, State, tribal and local law enforcement agencies

regarding lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities; 5) relations between law enforcement agencies and the communications industry to include leveraging existing and/or developing new private/public partnerships; 6) the development of standard practices within the law enforcement community; 7) implementation of CALEA; and 8) security and privacy policies, standards for participation by law enforcement agencies, and other issues relating to the functions, programs and operations of the NDCAC. The Board will further assist in shaping the goals and mission of the NDCAC by providing advice and guidance to the Director of the NDCAC on the establishment of policies and procedures designed to: ensure clarity in roles and responsibilities of the NDCAC; focus on established outcomes, intended results and accountability (by recommending specific courses of action); implement an effective infrastructure for the dissemination of technical information and methods; maintain an external focus to represent law enforcement stakeholders; pursue adequate resources necessary to accomplish the mission; and broker multi-agency participation and facilitate combined initiatives. The Board will provide insight into the diverse nature of jurisdiction-specific statutes and agency policies and procedures under which NDCAC participating law enforcement agencies operate. The Board will also receive information to review, monitor, and track training provided by or for NDCAC participating law enforcement agencies as well as recommend the development of standard practices for automated capabilities involving industry assistance.

4. **Description of Duties:** The Board will provide advice and recommendations to the Attorney General or the Attorney General's designated appointee on the selection of the

Director and Deputy Director(s) of the NDCAC. The Board also will provide advice and recommendations to the Attorney General or his designee and to the Director of the NDCAC as described in the Objectives and Scope of Activities of the Board, in Section

3. In addition, it will provide advice to the Attorney General on an annual basis, or more frequently as critical issues or events warrant, regarding: the technical challenges facing law enforcement agencies with respect to lawfully authorized electronic surveillance, collection of communications evidence, and technical location capabilities; programs, operations, systems and management of the NDCAC; the effectiveness of the NDCAC; and other issues relating to the core functions of the NDCAC. The duties of the Board are solely advisory in nature.

5. **Agency or Official to Whom the Committee Reports:** The Board will report to the Attorney General or the Attorney General's designee.
6. **Support:** The DOJ will provide all necessary support services for the Board.
7. **Estimated Annual Operating Costs and Staff Years:** The estimated annual operating costs of the Board and Subcommittees are expected to be approximately \$860,000. These costs include 3.5 work years of DOJ support services and the expenses of members to attend meetings.
8. **Designated Federal Officer:** A full-time or permanent part-time DOJ employee, appointed in accordance with agency procedures, will serve as the Designated Federal Officer (DFO). The DFO will have the authority to, at the request of the Board, establish Subcommittees. The DFO will approve or call all of the Board and Subcommittee meetings; prepare and approve all meeting agendas; attend all Board and Subcommittee meetings; adjourn any meeting when the DFO determines adjournment to

be in the public interest; and chair meetings when directed to do so by the Attorney General.

9. **Estimated Number and Frequency of Meetings:** The Board normally will meet at least semiannually, and Subcommittees will meet on an as-needed basis as determined by the DFO.
10. **Duration:** Continuing.
11. **Termination:** The Board's termination date is two years from the date this Charter is submitted to the Senate and House Judiciary Committees and is subject to renewal in accordance with Section 14 of FACA.
12. **Membership and Designation:** The Attorney General appoints all Board members. The Board consists of 15 voting members composed of Representative members, Regular Government Employees and/or Special Government Employees. The membership includes representatives from Federal, State, local and tribal law enforcement agencies. Additionally, there will be two non-voting Board members as follows: a federally-employed attorney assigned full time to the NDCAC will serve as a legal advisor to the Board, and the DOJ Chief Privacy Officer or his/her designee will ensure that privacy and civil rights and civil liberties issues are fully considered in the Board's recommendations. The Board will be composed of eight State, local, and/or tribal representatives and seven federal representatives. Any future changes to the voting membership of the Board will maintain the continued majority of State, local, and/or tribal representatives by one seat. The Board membership will be allocated as follows unless otherwise determined by the Attorney General:

**State, Local, and Tribal Law Enforcement:**

Of the eight seats reserved for State, local, and/or tribal representatives, seven seats shall be reserved for law enforcement officers who are agency heads such as a Chief of Police, Police Commissioner, Sheriff, Colonel, Superintendent, or other officially-designated executive for State, local, or tribal law enforcement. An eighth seat shall be reserved for a prosecutor from the State or local level. The Attorney General will consider nominations from the Association of State Criminal Investigative Agencies, the International Association of the Chiefs of Police, the Major City Chiefs, the Major County Sheriffs, the National Sheriff's Association, the National Narcotics Officers' Associations' Coalition, National District Attorneys Association, and the Association of Prosecuting Attorneys. The Board may identify other national law enforcement member organizations with relevance to NDCAC from which nominations can be proffered. The Attorney General shall ensure that one Board member is an executive from a law enforcement agency serving a jurisdiction of less than 500,000 persons, and that a second Board member is an executive from a statewide law enforcement agency (that may include both general police agencies [i.e., agencies which have both highway patrol and criminal investigation responsibilities] or investigative agencies in the service of State governments).

#### **Federal Law Enforcement**

- Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE) – may nominate individual(s) for one seat
- Drug Enforcement Administration (DEA) – may nominate individual(s) for one seat
- Federal Bureau of Investigation (FBI) – may nominate individual(s) for one seat
- Immigration and Customs Enforcement (ICE) – may nominate individual(s) for one seat



- United States Secret Service (USSS) – may nominate individual(s) for one seat
- United States Marshals Service (USMS) – may nominate individual(s) for one seat
- Any Federal law enforcement agency – may nominate individual(s) for one seat.

The membership of the entire Board will include active executive level officials (e.g., agency heads for State, local, or tribal representatives as described above; and members of the Senior Executive Service for Federal agencies) having responsibility for, or being substantially engaged in, the management of electronic surveillance capabilities, evidence collection on communication devices, and technical location capabilities from Federal, State, local and/or tribal law enforcement agencies from across the country. Board members must either have an appropriate level of security clearance or be eligible and able to obtain an appropriate level of clearance. Board members will serve two-year terms, and be eligible for reappointment if the Charter is renewed. Board members must attend all Board meetings. If a member fails to attend two meetings in the span of two years, regardless of proxy representation and absent mitigating circumstances, the member shall automatically relinquish membership on the Board. A Board member sending a proxy must notify the DFO of the Board in writing prior to the opening of the meeting for which the proxy is intended. The proxy must be from the same law enforcement organization (e.g., agency or association) as the individual represented, must be qualified for Board membership as described in paragraph 12 of this Charter, and may not be a current member of the Board.

**Executive Board Chairperson and Vice Chairperson**

The Board shall elect a Chairperson and Vice Chairperson at the first meeting following the Board's establishment, renewal, or reestablishment (i.e., after fulfilling FACA's charter filing requirements). The Chairperson and Vice Chairperson of the Board may be any Board member and the Vice Chairperson will assume all Chairperson responsibilities in the absence of the Chairperson.

To the extent determined necessary by the NDCAC, all Board members may be required to execute confidentiality/non-disclosure agreements prior to receiving access to government or industry proprietary information. This may be in addition to any requirements relating to members' security clearance.

13. **Subcommittees:** The overall advisory process structure may include Subcommittees.

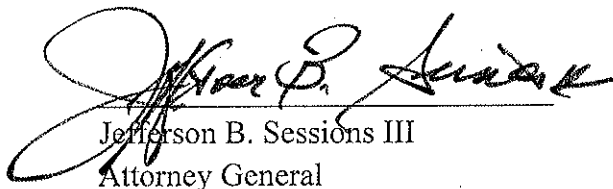
These Subcommittees will provide information and recommendations to the Board on technical and operational issues to assist the Board in carrying out its duties. The Subcommittees will report only to the Board and will not report directly to the Attorney General.

14. **Recordkeeping:** Records of the Board shall be handled in accordance with General Records Schedule 6.2. These records shall be available for public inspection and copying, subject to the Freedom of Information Act, 5 U.S.C. 552 and provisions governing the release or disclosure of Controlled Unclassified Information (CUI).

15. Filing Date: \_\_\_\_\_

Date

6/1/18

  
Jefferson B. Sessions III  
Attorney General